COMMENTS ON THE SOURCE COUNTRY INFORMATION SYSTEMS (SCIS) OF THE INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT (ICMPD)

May 2003

Protection Information Section
Department of International Protection
United Nations High Commissioner for Refugees
CP 2500, CH-1211 Geneva 2, Switzerland

E-mail: hqpr11@unhcr.org
Web Site: http://www.unhcr.org

COMMENTS ON THE SOURCE COUNTRY INFORMATION SYSTEMS (SCIS) OF THE INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT (ICMPD)

Table of contents

UNHCR, United Nations High Commissioner for Refugees
Department of International Protection, Protection Information Section

COMMENTS ON THE SOURCE COUNTRY INFORMATION SYSTEMS (SCIS) OF THE INTERNATIONAL CENTRE FOR MIGRATION POLICY DEVELOPMENT (ICMPD)

I. Introduction

1. On 7 June 2002, a meeting was held between UNHCR, ICMPD and the UK Home Office to discuss ICMPD's Source Country Information Systems (SCIS), known at that time as the Information Exchange System (IES).[1]

2. As a follow-up measure, it was agreed that UNHCR would carry out a detailed examination of SCIS procedures and recommend modifications that would allay various protection concerns UNHCR has about SCIS. On 22 June 2002, ICMPD forwarded to UNHCR the draft document *IES Overall Institutional and Operational Safeguards in Processing of Information Requests* in order to facilitate this review, the results of which are contained in the present note.

3. Each section of this note is subdivided as follows: (i) a summary of the relevant aspect of SCIS as understood by UNHCR; (ii) UNHCR's comments; and, as appropriate, (iii) UNHCR's recommendations. The focus is on the processing of individual information requests through SCIS in connection with asylum procedures and return and repatriation procedures, particularly requests involving the transfer of personal data. No analysis is made of other current SCIS outputs – namely, Municipality Information Fact Sheets, Topical Information Fact Sheets, Digital Photography Section and Personal Document Section – although UNHCR does not exclude commenting on these outputs at a later date.[2]

4. This note only addresses *generic issues* concerning the processing of individual information requests through SCIS. The implementation of SCIS in any particular country of origin, while based on standard SCIS methodology, is contextually unique. Specific SCIS country projects, existing or planned, are therefore not discussed, except insofar as they may help illustrate generic points.[3]

5. This note is not intended as a definitive or exhaustive statement by UNHCR on the processing of individual information requests through SCIS. Rather, its purpose is to further the ongoing and constructive dialogue on this issue between UNHCR, ICMPD, SCIS client governments and the European Commission.

II. Purpose of SCIS

A. Summary of SCIS

6. SCIS is based on the premise that "Source Country Information" is central to processing of asylum claims, and to procedures for voluntary and forced returns.[4] Accordingly,

> *"SCIS specializes in information requests seeking objective, factual information, by addressing these requests to leading agencies, experts and relevant organisations on the ground. Whether this information is required to assess the credibility of an asylum claim, or to facilitate a possible return/repatriation.*
>
> *SCIS provides legally safe answers, with information obtained in a neutral manner exclusively from open sources."*[5]

---

* Distribution outside UNHCR is restricted to ICMPD, SCIS clients and the European Commission.

[1] The note of the meeting is attached at Annex 1 below.

[2] UNHCR previously provided brief comments on these outputs in the specific context of the SCIS draft project proposal for Afghanistan. See UNHCR, *Comments on the ICMPD Source Country Information Systems (SCIS) draft project proposal for Afghanistan*, 21 February 2003.

[2] ICMPD-SCIS response to UNHCR's comments, 11 March 2003.

[3] Kosovo is currently the only location where SCIS is being implemented. Extension of SCIS to Sri Lanka was planned for autumn 2002, but has been delayed. A project proposal for extension of SCIS to Afghanistan was submitted to the European Commission and client States in spring 2003. SCIS standard methodologies have also been proposed for a Regional Property Information Exchange Mechanism between selected countries in south-eastern Europe. Feasibility studies for extension of SCIS to Northern Iraq and selected countries in Sub-Saharan Africa have also been mooted.

[4] ICMPD-SCIS, *SCIS at a Glance*, January 2003, p. 1.

[5] ICMPD-SCIS, *Information Request Guidelines*, January 2003 (6th edition), p. 3. See also ICMPD-SCIS, *SCIS at a Glance*, January 2003, p. 1: "Specifically, the programme's purposes are to foster informed decision making by government agencies

The term "legally safe answer" refers to

> *"the transparent process through which SCIS processes information requests. The SCIS obtains information exclusively from open sources; the information, and the means by which it is obtained, must be objective, verifiable and provided by official sources."*[6]

7. SCIS aims to respond to information requests within ten working days and, by November 2002, had processed more than 48,000 requests on behalf of 12 European governments. Approximately two thirds of these requests were related to the "independent verification of personal data or circumstances of one form or another,"[7] reflecting the fact that SCIS's focus is on "case-specific" country of origin information.[8]

8. There do not appear to be any statistics available on how many requests have related to refugees and asylum seekers.[9]

B. Comments

9. As recently observed by one refugee tribunal, "[a]ny information which is of potential assistance to the decision maker in carrying out what can sometimes be the extraordinarily difficult task of assessing a claimant's credibility is to be welcomed."[10] Indeed, access to accurate and reliable information is a condition *sine qua non* for identifying who is, and who is not, in need of international protection, as well as for developing strategies for solutions, including plans for voluntary repatriation. It can also assist in the development of an effective international response to general migration questions.[11] UNHCR therefore welcomes any initiatives that help States tackle these challenges, providing that such initiatives respect fundamental principles of human rights and refugee protection.

10. As States work to refine their information gathering systems, UNHCR has noticed a trend in recent years whereby some States, particularly in Europe, have increasingly been checking claims made by asylum seekers with information sources in the country of origin. Such checking may be carried out by a fact-finding mission despatched from the country of asylum, or directly by an embassy official on the ground. Alternatively, checking may be carried out by, for example, employing the research services of a local lawyer or of an independent organization. The information sources consulted may include, amongst others, private individuals, local non-governmental organizations (NGOs), international organizations (including UNHCR) and local and national authorities. The information sought may be general or particular, and may sometimes include information about specific individuals, including asylum seekers themselves.

11. Clearly, recourse to information sources in the country of origin can, in appropriate circumstances, be a useful means of helping to establish the facts of an asylum claim. Equally clearly, there is a need to ensure that national and international standards for the protection of personal data are observed, and that the security of asylum seekers and of their relatives and associates is not jeopardized through prejudicial disclosure. It is also essential to ensure the safety of the sources consulted, and not to undermine the safety and integrity of any ongoing humanitarian operations. The reliability of the information gathered is another critical issue and will depend *inter alia* upon the content of the question, how the question is asked, who the source of information is, how he or she perceives the questioner and the purpose of the question, why he or she chooses to respond and whether he or she may be under any pressure from any other quarters.

---

involved in all types of migration matters and by the refugees/returnees themselves by providing relevant information; expedite asylum procedures and humanitarian cases; administer background checks, verification of identity and personal circumstances."

[6] ICMPD-SCIS, *Information Request Guidelines*, p. 3.

[7] ICMPD-SCIS, *Migration and Security – the role of SCIS. Discussion Paper*, November 2002, p. 1.

[8] See, for example, ICMPD, *Introduction to the SCIS Information Request Processing Methodology*, November 2002, p. 1.

[9] SCIS's methodology precludes any central monitoring of the reasons why an information request is submitted, since clients are required to delete any information revealing the legal procedures that the individual concerned is undergoing in the host country.

[10] New Zealand Refugee Status Appeals Authority, Refugee Appeal No. 73545/02, 11 October 2002, paragraph 53.

[11] UNHCR, *Informed decision-making in protection: the role of information*, ExCom Sub-Committee of the Whole on International Protection, 27 September 1993.

12. Experience shows that a coherent body of country information requires multiple sources.[12] UNHCR recognizes that SCIS can be one such source, including in support of the refugee status determination (RSD) process,[13] but has concerns in relation to the protection of personal data, protection of personal safety, quality control, reliability of sources and the principle of equality of arms, as discussed in sections III to VI below.

III. Disclosure of personal data

A. Summary of SCIS

13. Information requests containing personal data – SCIS explicitly provides for the processing of information requests containing personal data. Examples include "verification of ethnicity", "information about someone's former whereabouts in their place of origin" and information about the "the current physical state of someone's house, by taking and forwarding a digital photograph to the end-user, or referring the question to a competent authority for an opinion".[14]

14. The SCIS checklist for clients[15] submitting requests containing personal data includes the following points: the name of the individual concerned; his or her date and place of birth; his or her date of departure and last known address in the country of origin; the names of his or her parents and their last known address.[16] The only personal data that is explicitly excluded from being processed through the SCIS is: information about the legal procedures that the individual is undergoing in the host country;[17] the name of the individual when only medical information is requested (although this does not exclude the individual's medical case history from being submitted as part of the request).[18]

15. Disclosure of personal data by the client to ICMPD – Clients submitting information requests containing personal data must, if their national legislation so requires, obtain the consent of the person concerned. However, if the client's national legislation does not require consent, ICMPD does not require it either. In such cases, ICMPD merely recommends that consent be obtained.[19]

16. The client should not include any personal data that is not necessary for processing the request.[20]

17. Disclosure of personal data by ICMPD to the SCIS sub-contractor – Receipt of an information request by ICMPD constitutes the client's authorization for ICMPD to disclose the request, and any personal data it contains, to the SCIS sub-contractor in the country of origin.[21] Where the disclosure of personal data is not necessary for processing the request, ICMPD will delete it before forwarding the request to the sub-contractor.[22] If the request mentions the legal procedures the individual is undergoing in the host country, ICMPD will delete this information as well.[23]

---

[12] *Ibid.*, paragraph 7.
[13] The term "refugee" is used in this paper in its broadest sense and extends to persons who might not necessarily meet the criteria for refugee status under the 1951 Convention/1967 Protocol relating to the Status of Refugees, but who nevertheless need international protection. See further UNHCR, *The International Protection of Refugees: Complementary Forms of Protection*, April 2001.
[14] *Information Request Guidelines*, p. 9.
[15] SCIS clients are governments and their designated agencies. All information requests submitted to SCIS should be channelled through a central "Request Processing Unit (RPU)" or focal point established by the client government for this purpose. It is foreseen that the RPU will actively screen the information requests and ensure that they are in conformity with the *Information Request Guidelines* and with the client country's data protection legislation (see *Information Request Guidelines*, p. 4)
[16] *Ibid.*, p. 16.
[17] *Ibid.*, p. 4 and 5.
[18] *Ibid.*, p. 11 and 17.
[19] In such cases, the client should state that it is acting in conformity with its national legislation. See *Information Request Guidelines,* p. 10; *Standard Contract with Client Governments* cited in *IES Overall Institutional and Operational Safeguards in the Processing of Information Requests*, p. 4.
[20] *Information Request Guidelines*, p. 4.
[21] *Standard Contract with Client Governments* cited in *Overall Institutional and Operational Safeguards*, p. 4.
[22] *Information Request Guidelines*, p. 9.
[23] *Information Request Guidelines.*, p. 5; ICMPD-IES, *Data and Requests Standard Operating Procedures*, 11th edition, June 2002, paragraph 2.4.3.

18. All communications between the SCIS Central Unit at ICMPD Vienna and the sub-contractor in the country of origin are encrypted. No personal data is included in the subject line of the email, as this part of an email is not encrypted.[24]

19. Disclosure of personal data by the SCIS sub-contractor to a third party – The sub-contractor may not provide its own answer to the request but is obliged to put the request to, and obtain an answer from, a third party ("contact person").[25] In principle, there are no restrictions concerning who the contact person may be.[26] For example, SCIS explicitly allows for disclosure of the request to government officials in the country of origin.[27]

20. Conclusions – All information requests accepted by ICMPD are forwarded to the SCIS sub-contractor and disclosed to one or more contact persons in the country of origin, even if, in the case of a request containing personal data, the individual concerned has not necessarily consented to disclosure to ICMPD and/or the sub-contractor and/or the contact person(s). The contact persons are selected by SCIS,[28] and in theory could be anyone whom the sub-contractor deems qualified to give an answer, including government officials.

21. Although the information request should not contain any reference to the reason why it has been submitted, the contact person(s) may well suspect that it concerns a refugee or an asylum seeker since the stated objectives of SCIS are to expedite asylum procedures and facilitate return procedures.

B. Comments

22. Refugee law and principles of data protection – UNHCR ExCom Conclusion No. 91 (LII) (2001) on Registration of Refugees and Asylum-Seekers stresses the "confidential nature of personal data and the need to protect confidentiality" whilst recognizing that the "appropriate sharing of some personal data in line with data protection principles can assist States to combat fraud, to address irregular movements of refugees and asylum-seekers, and to identify those not entitled to protection under the 1951 Convention and/or 1967 Protocol". The need to respect confidentiality applies to all stages of the asylum procedure, including if and when an application for refugee status is rejected.[29]

23. Confidentiality in asylum procedures is particularly important because of the vulnerable situation in which refugees and asylum seekers find themselves. For example, unauthorized disclosure of personal data to third parties in the country of origin or elsewhere could:

- Inhibit an asylum seeker from fully explaining his or her case, or even from making a claim for refugee status;[30]

[24] *Information Request Guidelines*, p. 4, 5 and 6; *Standard Operating Procedures*, section 2.3. Communications between the client and the Central Unit can also be encrypted at the client's request.
[25] See paragraph 54 below.
[26] Note that SCIS allows for a special procedure for any case deemed "sensitive" by the client (see paragraph 42 below). Note also that the subcontractor "shall refrain to communicate or disclose any information whatsoever related to information requests, except to those individuals directly contacted in order to answer an information request" (*Standard Contract with Implementing Partner (Sub-Contractor)* cited in *Overall Institutional and Operational Safeguards*, p. 17).
[27] As noted in paragraph 6 above, responses are to be obtained from "official" sources. The *Overall Institutional and Operational Safeguards* refer at p. 18-19 to "authoritative sources", including "officials" and "persons in authority". At the meeting with UNHCR on 7 June 2002, ICMPD acknowledged that personal data could be shared with the authorities of countries of origin (see note at Annex 1 below).
[28] *Information Request Guidelines*, p. 7: "Field Office staff need clearly formulated questions to allow them to identify the most suitable contact persons whom to address the questions to".
[29] UNHCR, *Asylum Processes (Fair and Efficient Asylum Procedures)*, Global Consultations on International Protection, Third Track – Executive Committee Meetings, EC/GC/01/12, 31 May 2001, paragraph 50(m): "The asylum procedure should at all stages respect the confidentiality of all aspects of an asylum claim, including the fact that the asylum-seeker has made such a request. No information on the asylum application should be shared with the country of origin." See also UNHCR, *Informed decision-making in protection: the role of information*, ExCom Sub-Committee of the Whole on International Protection, 27 September 1993, paragraph 8: "In developing and implementing an information strategy, UNHCR is […] conscious of the need to ensure that national and international standards for the protection of personal data are observed, and that individuals do not suffer loss of protection through prejudicial disclosure."
[30] See UNHCR, *Handbook on Procedures and Criteria for Determining Refugee Status*, paragraph 198: "A person who, because of his experiences, was in fear of the authorities in his own country may still feel apprehensive vis-à-vis any authority. He may therefore be afraid to speak freely and give a full and accurate account of his case." *Ibid.*, paragraph 200 :

- Endanger any relatives or associates of the asylum seeker remaining in the country of origin;
- Endanger the asylum seeker in the event of his or her return to the country of origin;
- Cause the asylum seeker to become a refugee "*sur place*".

Hence, while an asylum seeker has a duty to assist the examiner to the full in establishing the facts of his her case,[31] the examiner is not ordinarily entitled to disclose the asylum seeker's personal data to a third party.

24. Indeed, international data protection principles require that an individual consent to the sharing of his or her personal data with a third party unless there is an overriding interest at stake, either of the individual concerned, or of another individual or of society at large. Circumstances in which consent is not required are an exception, in which case disclosure must be necessary, in accordance with law, and proportionate to the legitimate aim pursued.[32] These principles are as applicable to aliens, including refugees and asylum seekers, as they are to the nationals of an asylum State.[33]

25. Personal data conveys information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.[34] An individual need not be explicitly identified for unauthorized disclosure of his or personal data to occur, and it must be ensured that particular asylum seekers cannot be *indirectly* identified through information gathering activities. The precise dividing line between data that is "personal" and data that is "anonymous" can be difficult to draw and, given the potentially serious prejudicial consequences of disclosure, great caution is called for when determining in a particular case that certain data is "anonymous". What may seem like an anonymous fact to an official in an asylum country could be quite the opposite when placed in context in the country of origin.

26. Data protection standards in the European Union – In view of the fact that the majority of SCIS clients are member States of the European Union (EU), and that the SCIS Central Unit at ICMPD Vienna is itself

"[…] It will be necessary for the examiner to gain the confidence of the applicant in order to assist the latter in putting forward his case and in fully explaining his opinions and feelings. In creating such a climate of confidence it is, of course, of the utmost importance that the applicant's statements will be treated as confidential and that he be so informed."

[31] UNHCR, *Handbook on Procedure and Criteria for Determining Refugee Status*, paragraph 205(a).

[32] A non-exhaustive list of international instruments concerning the right to privacy and/or the processing of personal data is attached at Annex 2 below.

[33] See the 1985 *United Nations Declaration on the Human Rights of Individuals Who are Not Nationals of the Country in Which They Live (1985)*, article 5(1): "Aliens shall enjoy, in accordance with domestic law and subject to the international obligation of the State in which they are present, in particular the following rights: […] (b) The right to protection against arbitrary or unlawful interference with privacy, family, home or correspondence". See further, for example, Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1980, article 1: "The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')." As stated in paragraph 26 of the *Explanatory report* on the 1980 Convention: "[…] The guarantees set out in the convention are extended to every individual regardless of nationality or residence. This provision is in accordance with the general principle of the Council of Europe and its member States with regard to the protection of individual rights. Clauses restricting data protection to a State's own nationals or legally resident aliens would be incompatible with the convention."

[34] Organization for Economic Cooperation and Development, *Explanatory Memorandum to the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)* (hereinafter "OECD Guidelines"), paragraph 41. See further *OECD Guidelines,* article 1(a): "'personal data' means any information relating to an identified or identifiable individual (data subject)"; Council of Europe, *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*, 1981, article 2(a): "'personal data' means any information relating to an identified or identifiable individual (data subject)"; *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (hereinafter the "Data Protection Directive"), article 2(a): "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors to his physical, physiological, mental, economic, cultural or social identity".

located in the EU, European legal standards for the protection of personal data are of particular relevance in the present context. Article 8 of the EU Charter of Fundamental Rights stipulates:[35]

> 1. *Everyone has the right to the protection of personal data concerning him or her.*
> 2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> 3. *Compliance with these rules shall be subject to control by an independent authority.*

Article 52(1) of the EU Charter adds:

> *"Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."*

27. Thus, although certain EU instruments in the field of asylum provide for the exchange of asylum seekers' personal data between participating States in order to determine the State responsible for examining an asylum claim, very strict limitations are placed on the personal data that may be disclosed, and on the modalities and purposes of disclosing it, when the exchange takes place without the consent of the persons concerned.[36] The various EU instruments in other fields of Justice and Home Affairs that provide for the exchange of personal data between States for certain purposes, similarly require that the exchange take place in conformity with national and international law, including international human rights standards.[37]

28. At a more general level, the "Data Protection Directive" (Directive 95/46/EC) establishes far-reaching standards under European Community law for the processing of personal data. According to the Directive, personal data may be processed only if the individual concerned has "unambiguously given his consent" or certain other conditions obtain.[38] The processing of special categories of personal data, namely data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and […] data concerning health or sex life", is expressly prohibited, save for certain exceptions such as the "explicit consent" of the individual concerned.[39] These special categories of data are, in certain instances, the very type of data that may typically be processed through SCIS.

29. The Data Protection Directive also requires Member States to permit transfers of personal data only to third countries outside the European Community where there is "adequate protection" for such data, unless one

[35] Although the EU Charter is not itself a legally binding instrument, its provisions concerning the protection of personal data are derived from certain other instruments that *are* binding. See Council of the European Union, *Charter of Fundamental Rights of the European Union: Explanations relating to the Complete text of the Charter*, December 2000, citing the following instruments in support of article 8 of the EU Charter: (i) Treaty establishing the European Community (Article 286); (ii) the Data Protection Directive; (iii) the European Convention on Human Rights (article 8); (iv) Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 1981.

[36] By definition, the participating States do not include the State of origin. See, in particular, Article 15 of the "Dublin Convention", the Council Regulations of 11 December 2000 and 28 February 2002 concerning "Eurodac", and Council Regulation 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national.

[37] See, for example, the 1995 Convention on the Use of Information Technology for Customs Purposes ("CIS Convention"), the 1995 Convention on the Establishment of a European Police Office ("EUROPOL Convention") and the Council Common Positions of 27 December 2001 on combating terrorism.

[38] Article 7, Data Protection Directive. Article 3(1) stipulates that the Directive "shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." Article 3(2) provides that the Directive shall not apply to the processing of personal data "in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V [provisions on a common foreign and security policy] and VI [provisions on police and judicial cooperation in criminal matters] of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing relates to State security matters) and the activities of the State in areas of criminal law."

[39] Article 8(1) of the Data Protection Directive. According to article 8(2)(a) of the Data Protection Directive, the laws of a Member State may provide that the prohibition on processing such special categories of data may not be lifted by the individual concerned giving his or her consent.

of a limited number of specific exemptions applies.[40] To date, the European Commission has recognized only Canada,[41] Hungary,[42] Switzerland[43] and the US Department of Commerce's Safe Harbor Privacy Principles[44] as providing "adequate protection". Otherwise, personal data may be transferred for processing to other countries only if:

- The individual concerned has given his or her "unambiguous consent", or another of the specific exemptions listed in article 26(1) of the Data Protection Directive applies; or

- The transfer is authorized, on a case-by-case basis, by a Member State and is notified to other Member States and the European Commission without any justified objection;[45] or

- The transfer is made under standard contractual clauses established by the European Commission for data transfers between data exporters established in the EU and data importers established in third countries.[46]

It should be noted that "processing" of personal data within the sense of the Directive by no means necessarily involves disclosure of the data to a third party.

30. The standard contractual clauses that have been established by the Commission for transfer of personal data to third countries include important safeguards for the individual. For example, if the transfer involves the "special categories" of data referred to above,[47] the data exporter must agree and warrant that the individual concerned has been informed or will be informed before the transfer that his or her personal data could be transmitted to a third country not providing adequate protection. Other safeguards for the individual include the entitlement to make inquiries and receive a response concerning the processing of his or personal data by the data importer, and the entitlement to enforce the contract as a third party beneficiary, including, in the event of a violation, entitlement to compensation for any damages suffered.[48] None of these clauses, insofar as they might have any relevance to SCIS, appear to be contained in the SCIS Standard Contract with Client Governments or the SCIS Standard Contract with Sub-Contractors.[49]

---

[40] Articles 25 to 26 of the Data Protection Directive. See further *Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC*; *Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of data to processors established in third countries, under Directive 95/46/EC*. See also United Nations, *Guidelines for the Regulation of Computerized Personal Data Files*, 1990, paragraph 9; Council of Europe, *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*, 1980, article 12; Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, 2001, article 2 (yet to enter into force).

[41] *Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*.

[42] *Commission Decision 2000/519/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary*.

[43] *Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland*.

[44] *Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*.

[45] Article 26(2) of the Data Protection Directive.

[46] Article 26(4) of the Data Protection Directive.

[47] See paragraph 28 above.

[48] See further *Commission Decision 2001/479/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC*; *Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC*.

[49] The standard contractual clauses under the Data Protection Directive are not listed in *IES Overall Institutional and Operational Safeguards in the Processing of Information Requests* (draft document), and so presumably are not contained in the SCIS Standard Contract with Client Governments or the SCIS Standard Contract with Sub-Contractors. The Standard Contract with Sub-Contractors refers to "the possible right of the person concerned to receive information on the processing of their personal data; and the possibility of monitoring the process by the relevant XXXXXX (enter client country) institutions", and states that "[i]n this regard, the contractors ensure that they will fulfil the minimum standards of XXXXXX

31. Conclusions – It is UNHCR's view that personal data of asylum seekers should in principle not be shared with the country of origin.[50] Where an asylum seeker believes that compelling evidence in his or her favour is obtainable from the country of origin, and that this evidence may be obtained only by disclosing certain of his or her personal data, he or she may request the authorities of the country of asylum for help in obtaining such evidence. However, it should not become a matter of routine for the authorities to seek the consent of asylum seekers to check their personal data in the country of origin. In addition to the considerations already discussed above, it should be recalled that, while the duty to ascertain and evaluate all the facts of a claim for refugee status is shared between the applicant and the examiner, refugee status determination is not an investigative procedure and the burden of proof in principle rests on the applicant.[51]

32. UNHCR recognizes that there may be exceptional cases of "over-riding interest" where the consent of an asylum seeker is not required to disclose certain of his or her personal data to the country of origin. In particular, UNHCR shares the legitimate concern of States that there should be no avenue for those supporting or committing terrorist acts to secure access to territory, whether to find a safe haven, avoid prosecution, or to carry out further attacks. The sharing of data between States is crucial to combating terrorism, and appropriate mechanisms need to be put in place in the field of asylum as in other areas. However, at the same time, care should be taken to ensure a proper balance with the refugee protection principles at stake. Thus, should it exceptionally be deemed necessary to contact the authorities in the country of origin, in case there is suspicion of terrorist involvement and the required information may only be obtained from these authorities, there should be no disclosure of the fact that the individual has applied for asylum.[52]

33. Outside the context of asylum proceedings, there may be certain situations where asylum seekers and refugees may quite naturally consent to sharing certain of their personal data with the country of origin. For example, some personal information will need to be shared, subject to the consent of the persons concerned, with the authorities of the country of origin in the context of organized voluntary repatriation arrangements, or to facilitate family reunification, transfer of assets, or voter registration and election procedures.[53]

34. Regarding persons found not to be in need of international protection, the limited sharing of personal data with the authorities of the country of origin can be legitimate in order to facilitate return, even if this is without the consent of the individuals concerned. Such cases usually arise when nationality is in question and/or the individual has no national travel or identification documents. However, disclosure should go no further than is lawful and necessary to secure readmission, and there should be no disclosure that could endanger the individual or any other person,[54] not least disclosure of the fact that the individual has applied for asylum. Moreover, everything should be done in the first instance to secure the voluntary nature of return.

C. Recommendations

35. A precondition to the processing of personal data through SCIS should be the consent of the individual concerned unless, exceptionally, a legitimate over-riding interest is at stake. As SCIS is currently conceived, this means that the individual should consent to the following:

    - The disclosure of his or her personal data to ICMPD;[55]

(enter client country) data protection laws)". Similar provisions are contained in the Standard Contract with Client Governments. See *Overall Institutional and Operational Safeguards*, p. 6 and 17.

[50] See note 29 above.

[51] See further paragraph 196 of the UNHCR *Handbook on Procedures and Criteria for Determining Refugee Status*.

[52] UNHCR, *Addressing Security Concerns without Undermining Refugee Protection*, Rev.1, November 2001, paragraph 11.

[53] Only necessary information should be released, e.g. in the context of organized voluntary repatriation, information that is necessary to obtain clearance for administrative formalities or in order to benefit from amnesty guarantees.

[54] See further section IV below.

[55] At the Seventh Joint Meeting of SCIS Client Governments in Vienna in February 2003 it was suggested that one Client Government might be able to forward information requests to SCIS on behalf of other Client Governments. If the request contained personal data, the forwarding of this data from one client to another would require the consent of the individual concerned.

- The onwards transfer of his or her personal data (i) outside the EU (ii) to the sub-contractor in the country of origin;

- The disclosure of his or her personal data by the sub-contractor to the contact person(s) on the ground.[56]

Consent must be freely given, explicit and unambiguous, and fully and properly informed. Any conditions imposed by the individual should be respected, such as any restrictions concerning the permitted extent of disclosure of his or her personal data and the contact persons to whom disclosure may be made.

36. There is obviously no need for consent if an information request contains data that is "anonymous", as opposed to "personal". However, separating the "anonymous" from the "personal" is not necessarily a straightforward matter, especially in the context of a foreign country and culture. As mentioned above, what may seem like an anonymous fact to an official in an asylum country could be quite the opposite when placed in context in the country of origin.

37. In certain cases, an asylum seeker may actually request that his or her personal data be "verified" in the country of origin. However, States should not as a matter of routine seek the consent of asylum seekers to check their personal data in the country of origin. Should consent be sought and withheld, this should not lead in and of itself to any adverse inferences about the applicant's credibility.

38. The question whether it may be appropriate and lawful to channel an information request containing personal data through SCIS in order to facilitate the return of a person found not to be in need of international protection can only be answered in the circumstances of the individual case. In the event that the individual does not consent to the processing of his or her personal data, factors to be taken into consideration in addition to those already mentioned in paragraph 34 above include the identity of the contact person(s) to whom the personal data would be disclosed, and the specific purpose of such disclosure. Ordinarily, the most appropriate channel of inquiry will be direct bilateral communications between the two States concerned.

39. Special safeguards may need to be included in SCIS contracts with clients and sub-contractors in view of the fact that personal data does not generally enjoy the same legal protection in other parts of the world as it does in the EU. Such safeguards could also ensure that any European Commission funding of SCIS would not inadvertently undermine the letter, object and purpose of the Treaty establishing the European Community, article 286 (ex-article 213b) of which provides that:

> *"From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty."*[57]

IV. Risk to personal security

A. Summary of SCIS

40. Security of SCIS staff and contact persons – SCIS will not process any information request that could endanger the security of staff, contact persons or their relatives and associates.[58]

41. SCIS permits disclosure to the client of the identity of the contact person(s) involved in providing the response to a particular information request.[59] However, the client may not disclose these details to the individual with respect to whom the request was made (whether the request contained any personal data or

[56] At present, SCIS prohibits disclosure of the identity of contact persons to the individual who is the subject of the information request. Under these circumstances, the individual concerned may therefore decide to prohibit the disclosure of his or her personal data to the contact person(s). See further paragraphs 41, 69 to 70, 77, and 83 to 84 below.
[57] See also *Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies on the free movement of such data.*
[58] *Information Request Guidelines*, p. 4; *Overall Institutional and Operational Safeguards*, p. 17 to 18.
[59] See paragraph 69 below.

not) since this could "potentially compromise [staff and contact] persons, their relatives and associates, and the successful continuation of the project".[60]

42. Security of other persons – In acknowledgement of the fact that the disclosure of personal data could have serious consequences for individuals who are the subject of information requests, or for their relatives and associates, SCIS provides for the following procedure in cases that the client deems "sensitive":

> *"Without sending us personal data, but only the exact location where the investigation should be carried out, the SCIS Central Unit would send you [the client] a report from the field explaining how we would propose to deal with the investigation of this particular information request. A short report detailing which agencies and individuals we would contact in order to answer the request would be sent to you. You would then be in a position to make an informed decision whether to go on or not with the actual request."*[61]

43. The client retains sole discretion whether to proceed with the request, and is considered to be solely responsible for all requests containing personal data that are processed through SCIS.[62]

44. Conclusion – SCIS assumes full responsibility towards staff and contact persons but apparently exonerates itself from responsibility towards individuals who are the subject of information requests.

B. Comments

45. In UNHCR's own practice, staff must ensure that the sharing of information (general or personal) will not put *any* individual at risk, and that it will not jeopardise the organization's country operations. For example, even if a refugee or asylum seeker consents to share his or her personal data with a third party in the country of origin for a certain purpose, UNHCR staff are required to bear in mind that, depending on the country situation, information sharing with, *inter alia*, local NGOs or local staff of international NGOs may be problematic because their vulnerability may render them more exposed to pressure from State authorities, secret services, or other interested third parties.

46. The information checking that may be carried out by foreign embassies in countries of origin is fundamentally different in its approach from SCIS. For example, it tends to be low-key and has the advantage that the staff concerned are protected by diplomatic status and immunity, and so are less susceptible to any local pressures. By contrast, SCIS is a high-profile, high-turnover operation, whose staff do not necessarily enjoy the same immunity. Local perceptions of SCIS are therefore likely to have a significant bearing on safety matters. If the SCIS sub-contractor is an organization belonging to the humanitarian community, these perceptions could extend, by association, to the humanitarian community as a whole.

47. Given that SCIS acts on behalf of foreign governments, and that one of its express purposes is to administer background checks on individuals,[63] local perceptions could be negative in some quarters.[64] This could especially be the case in countries emerging from a conflict situation or otherwise suffering from internal

[60] *Information Request Guidelines*, p. 8.
[61] *Ibid.*, p. 10.
[62] *ICMPD-IES/UNHCR Meeting Report*, Vienna, 7 February 2002. The *Information Request Guidelines* are not entirely consistent on this point. See p. 9: "Nevertheless, there may be occasions where the information requests cannot be answered for a number of reasons: the disclosure of personal data can compromise the security of the person concerned […]". However p. 10 goes on to say: "the security and physical integrity of the staff […] remains the foremost concern."
[63] See note 5 above.
[64] See SCIS's own findings, *KIP Field Mission August 2002 – Summary Report*, August 2002, p. 2 to 3: "The most striking finding of this mission was how little knowledge staff of international agencies in Kosovo have about KIP, after 2 years of operations and 40,000 Information Requests processed. This lack of knowledge of what the purpose of KIP is, who stands behind it and what its methodology and limitations are, *especially the limitation to providing exclusively information which is available from open sources and within the public domain*, are leading to a distorted perception: **KIP is at times viewed with suspicion**, sometimes even perceived as a kind of secret service. This renders investigations for Information Requests often difficult, sometimes impossible (e.g. with KFOR, UNMIK Police). […] To counteract this misperception of KIP, very **intense liaison work** is necessary" [emphases in the original].

instability. Any such negative perceptions could be exacerbated if SCIS were to diversify into providing background information for security screening of individuals, as has recently been mooted.[65]

C. Recommendations

48. An information request should not be processed if this would result in a reasonably foreseeable risk to the security of *anyone*, whether associated with SCIS or not. A responsibility and, as the case may be, legal duty of care is owed to:

- The individual with respect to whom the request is made, and his or her relatives and associates;
- SCIS staff and contact persons, and their relatives and associates;
- Humanitarian personnel in general;[66]
- Other persons as applicable.

49. In some country situations, it might be safest for SCIS not to process any personal data at all.

V. Answering the information request in the field

A. Summary of SCIS

50. Request Template – The SCIS Central Unit in Vienna extracts the questions from the client's information request, translates them as necessary and transfers them onto a Request Template, which is then sent back to the client for comments and approval. If the client does not respond within 24 hours, the Request Template is deemed to be approved.

51. Once approved, or deemed to be approved, the Request Template is forwarded to the sub-contractor in the field. It should contain no means of identifying the client country concerned.[67]

52. Time-limit for answering information requests – In principle, information requests should be answered within ten days of being forwarded to the field, although this timeframe may vary.[68] If the request cannot be answered within the required timeframe, the responsible Field Office must provide an explanation for the delay.[69] If after 30 days an answer has still not been obtained, the client will be offered a partial answer (if available) or will be invited to abandon the request.[70]

53. Internal Answer Template – Upon receipt of the Request Template, the sub-contractor should assign it to a Field Office, which should then transfer the information request onto an Internal Answer Template for investigation by staff.[71] At the end of the investigation, the Internal Answer Template should contain answers to all of the client's questions, the details of all the contact persons met, and the date, time and location of the interviews carried out by the staff concerned. The staff themselves should be identified by a code name.[72]

54. Answering the request – Staff are restricted to obtaining a statement of fact from the contact persons consulted and should not provide their own answers to the client's questions.[73] The contact persons should

[65] ICMPD-SCIS, *Migration and Security – the Role of SCIS. Discussion Paper*, January 2003, p. 1.
[66] Note the duty to ensure the safety and security of United Nations and associated personnel stipulated in article 7 of the *UN Convention on the Safety of United Nations and Associated Personnel*, 1994.
[67] *Information Request Guidelines*, p. 6 to 7; *Standard Operating Procedures*, 2.4.1 to 2.4.16. The questions may be reformulated in the process of being transferred to the Request Template, and SCIS may also suggest other questions to the client.
[68] *Information Request Guidelines*, p. 3.
[69] *Standard Operating Procedures*, 2.4.
[70] *Ibid.*, 2.5.
[71] *Ibid.*, 2.4.22 to 2.4.24
[72] *Ibid.*, 2.2
[73] *Ibid.*, 2.4.31: "All the information must be sourced to the organization or person providing it. At no time shall the IES provide its opinion or analysis on any given subject, or be the body providing the answer." See also ICMPD-SCIS, *Introduction to the SCIS Information Request Processing Methodology*, November 2002, p. 1.

be selected from among the "leading agencies and institutions in the field of the information request".[74] Their answers should be "clear, concise, and […] not leave any room for interpretation".[75]

55. Staff should take a copy of the Internal Answer Template with them to each interview and inform the contact person that they will take notes on this template. At the end of the interview, the contact person should review the Internal Answer Template and confirm verbally that it reflects the answer he or she gave.[76]

56. Staff can return an information request if any clarification is needed from the client.[77]

57. Verification of the answer for completeness and accuracy – The sub-contractor's Field Project Manager should "verify" the answer "for completeness, accuracy and internal integrity" before sending the Internal Answer Template to the SCIS Central Unit in Vienna.[78] The Central Unit should "edit" *[sic]* the answer and carry out the same verifications for completeness, accuracy and internal integrity as the Field Project Manager.[79] Any answer that is "questionable for a valid reason (wording, typos, contradictory or inconsistent with a previous answer on the same topic, incompleteness, unclear, etc.)" should be sent back to the previous step in the chain.[80]

58. In November 2002, SCIS claimed that it had by then processed over 48,000 information requests without any verified errors:

> *"SCIS methodology is characterised by rapid sourcing of targeted, factual field-based information, providing short response times, and standard high quality answers in a neutral, objective and transparent manner. This SCIS process is not designed to be adversarial, as the information obtained is meant to be purely factual and shared with the person concerned; thereby providing an effective feedback mechanism and a safeguard against possible error. Through the strict application of this methodology, SCIS has processed more than 48,000 information requests so far without any verified errors."*[81]

59. Conclusions – SCIS does not answer the information request itself; instead, it seeks to identify one or more authoritative contact persons willing and able to provide an answer that can be relayed to the client. SCIS effectively plays the role of an intermediary since the answer to the information request is attributed to the contact person(s), not to SCIS.

B. Comments

60. The approach of SCIS may be contrasted, for example, with that of a human rights organization. Human rights organizations tend to report at a level of generality, to reach conclusions only after consulting, cross-checking and evaluating numerous different sources of information, and to go no further than making a series of allegations accompanied by a call for an investigation. SCIS, on the other hand, responds to isolated queries, may base its responses on the answer of only one person, does not evaluate this answer (except formalistically as in paragraph 57 above) and yet effectively claims to present "facts".

61. However, the challenges of obtaining accurate information in the field are myriad. To take one example by way of illustration, the following questions and answers in the SCIS Afghanistan feasibility study are worthy of note:

---

[74] *Information Request Guidelines*, p. 8.
[75] *Ibid.*, p. 8.
[76] *Standard Operating Procedures*, 2.4.31 to 2.4.32; *Information Request Guidelines*, p. 8.
[77] *Standard Operating Procedures*, 2.4.21, 2.4.25 to 2.4.28. Staff may also return an information request if it raises security concerns.
[78] *Standard Operating Procedures*, 2.4.35 to 2.4.37; *Information Request Guidelines*, p. 8.
[79] *Standard Operating Procedures*, 2.4.39; *Information Request Guidelines*, p. 8.
[80] *Standard Operating Procedures*, 2.1.2 to 2.1.3, 2.4.39.
[81] ICMPD-SCIS, *Introduction to Information Request Processing Methodology*, November 2002, p. 1.

Question:

"Are there any project specific constraints in Afghanistan in general or in your FO/AoR in particular which you would like to highlight at this time? This especially regarding the collection of certain types of public, open source, factual information (e.g. no information source available, information source reluctant to pass on information, fees or special procedures imposed, other) as shown in the sample requests that are attached to this questionnaire."

Answer:

"Widespread corruption is a problem, and contact person fatigue could well be if repeatedly asked the same questions. No further problems, apart from topical questions below."[82]

The topical question relating to "confirmation of personal data, circumstances, ethnic origin" was answered as follows:

"Lack of registers will in most case leave only the option of confirming personal data, circumstances and ethnic origin through community based contact persons. In the rural areas the Malekhs, appointed persons representing the population in front of the authorities, could provide all such information if willing to. In urban areas there are usually no Malekhs having this sort of liaison function, but government-appointed representatives who do not necessarily live in the neighbourhood and who thus usually have less thorough knowledge of the population. Both in rural and urban areas the Mullahs will have thorough knowledge of the population. Establishment of good working relationships with these contact persons will require careful choice of investigating staff (age, ethnic origin, clan, family, communication skills) and some proof of respect (meeting with Head of FO, guest present, invitation) though not necessarily bribery."[83]

62. The feasibility study hence concluded *inter alia* that:

"One issue which must be noted is the (complete or partial) lack of accurate registries and official records; most either non-existent, or having been removed, destroyed or not maintained over the last 20 years. This lack of records can in part be made up for by the personal knowledge that community leaders (mullahs, malekhs and similar elected or government appointed community representatives) have of their neighbourhood and its population (for requests related e.g. to residence, kinship, personal circumstances). Talks held in Afghanistan and experience from the SCIS Kosovo (KIP) suggest that such community leaders constitute a valuable information source. For some AoR parts, however, there may be no community representatives or they may be reluctant to give information. Networking capacities at all levels will be required for the identification and maintenance of these information sources."[84]

63. While SCIS aims to select contact persons from among the "leading agencies and institutions in the field of the information request", it should be noted that selection of sources is rarely neutral and may well imply a value judgement closely linked to interpretation of the situation on the ground. Moreover SCIS staff may also, consciously or unconsciously, be subjected to potential personal, professional or political pressure to consult certain sources and not others; for example, the most reliable sources are not necessarily those which provide the fastest answer. There are also numerous reasons why the sources selected may not necessarily give an accurate or complete answer; for example, they may be under conscious or unconscious pressures of their own, be prejudiced or biased, be dishonest, be mistaken, exaggerate, and/or not necessarily have any direct knowledge of the point on which they answer. They may respond with a statement of fact when actually they have only an opinion on the point in question, or they may even simply try to please by inventing an answer to a point concerning which they have no knowledge or opinion at all.

64. SCIS aims to maximize the objectivity of the responses provided by ensuring that neither field staff nor the contact persons are aware of the specific reason for the information request, nor even of the country from

[82] SCIS, *Key Operational Questions for SCIS Afghanistan with Input by IOM Afghanistan, (undated)*, p.4.
[83] *Ibid.*, p.5.
[84] SCIS, *Source Country Information Systems (SCIS) Afghanistan Feasibility Study. Terms of Reference – Answered*, (undated), p. 6

which it emanates.[85] However, while this may help reduce the potential for an agenda-driven answer, it by no means eliminates it. As already mentioned above,[86] contact persons could reasonably speculate that an information request concerns a refugee or asylum seeker, and perhaps try to give an answer which they believe might either favour or prejudice the person concerned. They might also have other reasons for giving answers that are less than frank. For example, in answer to a question relating to the availability of local services (such as health care or temporary accommodation facilities) contact persons might conceivably deliberately underplay any problems out of community pride or, alternatively, exaggerate the situation in an attempt to attract international aid and development assistance. The same question could even be answered by the same person in different ways, depending on who asks it.

65. It is also widely recognized in information gathering operations that many people believe that to have many "don't know" answers makes them look bad, and hence may exert a high level of effort to get respondents to make a choice. The risk of this may be higher in a situation where answers have to be obtained within a short timeframe, and where useable answers are considered as only those which do not leave any room for interpretation.
66. This is not to suggest that other information gathering systems do not face similar challenges to SCIS, but simply to caution against overconfidence in the accuracy of the information obtained, particularly if it is based only on "official" sources or on the answer of only one person.

C. Recommendations

67. SCIS standard operating procedures do not appear to include a protocol for taking statements from contact persons, other than the procedure summarized in paragraphs 54 to 55 above. UNHCR recommends the introduction of a comprehensive and explicit protocol, which should include as a minimum the following points:[87]

- The interview should be held in private, so that any personal data disclosed to the contact person is not disclosed to other persons as well, and so that the contact person is able to speak as freely as possible without being influenced by others;

- Staff should introduce themselves and explain SCIS and the purpose of the interview;

- In explaining the purpose of the interview, it should be made explicit that the answers given may be tendered in evidence in legal proceedings in a foreign country, and that it is important that the contact person answers truthfully;

- The contact person should give his or her consent for the interview to proceed, and be asked whether he or she consents to his or her answers being used in legal proceedings and his or her identity being disclosed to the parties concerned;[88]

- Staff should be careful not to ask leading questions or to inadvertently influence answers in any other way, regardless of time or any other pressures;

- The contact person should sign (not just verbally confirm) his or her statement to confirm that it is true to the best of his or her knowledge and to impress upon him or her a sense of accountability for its content;

[85] See, in particular, *Information Request Guidelines*, p. 5: "The reason for this operation is to ensure the utmost objectivity and transparency in the processing of any information request by removing any information that could be construed as agenda-driven, or leading to bias. The IES Central and Field Units staff members do not need to know whether the purpose of the questions concerns a refugee trial, an appeal, or an impending repatriation. By removing this type of information, you ensure that no one involved in the process of the answering of the request could in any way be prejudiced or biased; it also produces the same result with any outside party that may later be involved with the result of the information request, as it can be clearly demonstrated that the request was processed in the most open, objective and transparent manner."
[86] See paragraph 21 above.
[87] UNHCR is unaware of the extent to which some of these points may be covered during the training of staff, but it is also important that they be included as part of written procedures.
[88] At present, the SCIS norm is that the identity of the contact person may only be revealed to the client. See paragraphs 69 to 70 below.

- Contact persons should not be remunerated, either in cash or in kind, except in payment of any standard administrative fees for official services lawfully rendered (e.g. State notary services), or in reimbursement of any legitimate expenses incurred (e.g. travel expenses of private persons).

68. SCIS sub-contractors and their staff should be selected so as to eliminate as far as possible any risk of them being exposed to undue pressures or conflicts of interest.

VI. Application of the response to the information request

A. Summary of SCIS

69. External Answer Template – The SCIS Central Unit is required to prepare an External Answer Template based on the Internal Answer Template received from the field. The External Answer Template reproduces all the questions and answers contained in the Internal Answer Template, but all means of identifying the responsible staff members and contact persons are removed. Both the Internal Answer Template and the External Answer Template are then sent to the client.[89]

70. Clients are *recommended* to share the External Answer Template with the individual concerned (hereinafter "the applicant") and his or her legal representative. However, clients may not disclose the Internal Answer Template publicly, including in judicial proceedings, not even just to the applicant and his or her representative, unless SCIS agrees in writing that an exception may be made in the individual case.[90] As mentioned above, this is because disclosure could "potentially compromise [staff and contact] persons, their relatives and associates, and the successful continuation of the project".[91]

71. Clients are encouraged to react to any feedback provided by the applicant and to send as many follow-up or clarification requests as they wish.[92]

72. Conclusions – The applicant enjoys "equality of arms" with the client concerning disclosure of the contact person's answers, but not concerning disclosure of the contact person's identity.

B. Comments

73. The nature of refugee status determination proceedings – Frequently the only information available in RSD proceedings is the applicant's oral testimony, any personal documents he or she submits, and information relating to general country conditions, such as human rights reports. The latter rarely provides the kind of detail that would be necessary to fully corroborate an individual claim and, as stated in UNHCR's *Handbook on Procedures and Criteria for Determining Refugee Status*,

> *"203. […] it is hardly possible for a refugee to 'prove' every part of his case […] indeed, if this were a requirement the majority of refugees would not be recognized. It is therefore frequently necessary to give the applicant the benefit of the doubt.*
>
> *204. The benefit of the doubt should, however, only be given when all evidence has been obtained and checked and when the examiner is satisfied as to the applicant's general credibility. The applicant's statements must be coherent and plausible, and must not run counter to generally known facts."*

74. UNHCR recognizes the attraction of systems such as SCIS which aim to provide detailed information that may help test an applicant's story and therefore narrow any margin of doubt. However, as discussed below, the evidential weight of SCIS responses in legal proceedings needs to be assessed with great care, particularly if the response relates to a material issue, such as the identity of the applicant, and there appears to be a gap or discrepancy between the response and the facts as claimed by the applicant.

---

[89] *Standard Operating Procedures*, 2.2, 2.4.40 to 2.4.43
[90] *Information Request Guidelines*, p. 8; *Overall Institutional and Operational Safeguards*, p. 24 to 25. The latter document recommends on p. 24 that the ***Internal*** Answer Template be shared with the applicant. The substitution of "external" by "internal" is clearly a typographical mistake.
[91] See paragraph 41 above.
[92] *Information Request Guidelines*, p. 9.

75. Disclosure of information and its sources – UNHCR has long been committed to the use of publicly available information as a basis for decision-making. Such information, if gathered and used on the basis of coherent standards, has the advantage of being open to review and verification.[93] UNHCR accordingly considers that information and/or its sources may be withheld only as an exception and under clearly defined conditions where the disclosure of sources would seriously jeopardize national security or the security of the organizations or persons providing the information.[94]

76. SCIS is at variance with these principles because it presumes that the security of contact persons and country operations is always at stake and imposes the anonymity of sources as a norm. Instead of justifying in an individual case why the Internal Answer Template should not be disclosed to the applicant, SCIS shifts the burden to the client to justify why, as an exception, the Internal Answer Template should be disclosed. Disclosure remains purely at the discretion of SCIS. Although in theory a national court could order the client to disclose the Internal Answer Template to the applicant, in practice this would frustrate the contract between the client and SCIS and would presumably result in the contract's termination, or at least in SCIS no longer forwarding the Internal Answer Template to the client.

77. In cases where the consent of the applicant is required for the processing of the information request because it contains his or her personal data, the applicant might prohibit the disclosure of his or her personal data to any contact person who is not willing to disclose his or her own identity in return. However, the applicant does not have this possibility in cases where the information request does not contain personal data.

78. The non-disclosure of the Internal Answer Template is prejudicial to the applicant because, as long as the contact person providing the answer remains anonymous, the applicant cannot challenge his or her credentials as an allegedly reliable and authoritative source in his or her particular case.

79. Hearsay evidence – SCIS is a system that utilizes hearsay evidence, that is evidence which does not represent the actual knowledge or opinion of SCIS, but is only a recitation of what SCIS has been told by the contact person either orally or in writing. Although rules of evidence, for good reason, are often not as strict in RSD proceedings as they are in other legal proceedings, and hearsay evidence may frequently be introduced and given weight as part of an asylum seeker's testimony,[95] it can be a different matter entirely if such evidence is introduced for purposes of testing the asylum seeker's credibility.

80. Whether such evidence has significant probative value depends very much on its provenance and/or on whether all parties to the proceedings agree to accept it. For example, reports of well-known international human rights organizations are relied upon extensively in RSD proceedings even though, as documents, they constitute hearsay, and they are also frequently based on anonymous sources. Such reports are generally accepted without their authors being asked to give evidence in person because the organizations concerned are known for their independence, impartiality, authority and reliability – and because the reports go through a process of rigorous review prior to publication, resulting in the unequivocal support of the organizations concerned for the findings, assessments and analysis they contain.

81. By contrast, SCIS shifts all responsibility to the client for evaluating and interpreting the "raw data" constituting the answers collected from the contact persons in the field. The evaluation is hampered by the fact that neither the client nor the applicant can directly question the contact persons about their answers. If a contact person represents an international organization known for its independence, impartiality and reliability, and answers an information request in his or her official capacity, then the parties to the proceedings may be inclined to accept his or her answer without question. However, uncritical acceptance by all of the parties is much less likely if the contact person is a local government official. Although in principle the contact person could be "examined" or "cross-examined" by means of further information requests being sent through SCIS, the probative value of such a procedure is in no way comparable to that

[93] UNHCR, *Informed decision-making in protection: the role of information*, Sub-Committee of the Whole on International Protection, 27 September 1993, paragraph 7.
[94] UNHCR, *Summary Observations on the Amended Proposal by the European Commission for a Council Directive on Minimum Standards on Procedures in Member States for Granting and Withdrawing Refugee Status (COM(2000) 326 final/2, 18 June 2002)*, January 2003.
[95] For example, an asylum seeker's fear of persecution may arise due to threats voiced by other persons.

of a witness giving testimony under oath on the spot unchecked by barriers of distance, time and anonymity.

82. Conclusions – UNHCR does not wish to convey the impression in the above that it considers that the majority of SCIS responses to information requests to date have been inaccurate or misleading. However, no matter how reliable responses may be *in general*, the key question is "how reliable is *this* response in *this particular* case?". As SCIS itself acknowledges, the way an information request is formulated "can influence the result and the process dramatically".[96] If the applicant disagrees with the response, he or she is prejudiced by the fact that the response is anonymous and hearsay. The "inequality of arms" caused by the fact that the identity of the contact person is known to the client is another source of potential prejudice.

C. Recommendations

83. SCIS methodology should be based on the principle of "equality of arms". The identity of the contact person should be disclosed either to both the client and the applicant, or to neither. Since SCIS responses to information requests are meant to be obtained exclusively from "open sources",[97] disclosure should be the norm.

84. In exceptional cases, a client may seek unilateral disclosure of a contact person's identity. Any decision to release the identity of the contact person only to the client, and not to the applicant as well, could only be on security grounds and should be clearly motivated and be subject to independent review.

85. The evidential weight of SCIS responses to information requests should be assessed with caution, particularly if the response relates to a material issue, such as the identity of the applicant.

86. Public scrutiny can be a useful means of quality control and responses to information requests which do not contain personal data should therefore be made publicly available on the SCIS website. UNHCR previously recommended publication of SCIS responses to information requests in the specific context of the SCIS draft project proposal for Afghanistan,[98] and welcomes the fact that SCIS has agreed to this providing that clients agree as well.[99]

87. If the client is unable to use a response to an information request because the identity of the contact person is non-disclosable, the client may still be able to use the response as an indicator for seeking out a source which is disclosable.

88. If SCIS engaged in fact-finding, instead of merely acting as an intermediary between contact persons and clients, this could increase the evidential weight of SCIS responses to information requests. In many cases, it could also make the disclosure of the identity of contact persons unnecessary.

VII. Conclusions

89. UNHCR recognizes the challenges involved in designing and implementing a field-based information system aimed at processing large numbers of information requests within a very short timeframe. The Office appreciates this opportunity to comment on SCIS methodology, and hopes that its recommendations will be seen as being both constructive and practical. These recommendations, consolidated from the text above, are as follows:

A. Protection of personal data

1. A precondition to the processing of personal data through SCIS should be the consent of the individual concerned unless, exceptionally, a legitimate over-riding interest is at stake. As SCIS is currently conceived, this means that the individual should consent to the following:

[96] *Information Request Guidelines*, p. 16.
[97] See paragraph 6 above.
[98] UNHCR previously made this recommendation in *Comments on the ICMPD Source Country Information Systems (SCIS) draft project proposal for Afghanistan*, 21 February 2003.
[99] ICMPD-SCIS response to UNHCR's comments, 11 March 2003.

- The disclosure of his or her personal data to ICMPD;
- The onwards transfer of his or her personal data (i) outside the European Union (ii) to the SCIS sub-contractor in the country of origin;
- The disclosure of his or her personal data by the sub-contractor to the contact person(s) on the ground.

Consent must be freely given, explicit and unambiguous, and fully and properly informed. Any conditions or restrictions imposed by the individual should be respected.

2. There is no need for consent if an information request contains data that is "anonymous", as opposed to "personal". However, separating the "anonymous" from the "personal" is not necessarily a straightforward matter, especially in the context of a foreign country and culture. What may seem like an anonymous fact to an official in an asylum country could be quite the opposite when placed in context in the country of origin.

3. In certain cases, an asylum seeker may actually request that his or her personal data be "verified" in the country of origin. However, States should not as a matter of routine seek the consent of asylum seekers to check their personal data in the country of origin. Should consent be sought and withheld, this should not lead in and of itself to any adverse inferences about the applicant's credibility.

4. The limited sharing of personal data with the authorities of the country of origin can sometimes be legitimate in order to facilitate the return of persons found not to be in need of international protection, even if this without the consent of the persons concerned. Such cases usually arise when nationality is in question and/or the individual has no national travel or identification documents. However, disclosure should go no further than is lawful and necessary to secure readmission, and should not reveal any information, including the fact that the individual applied for asylum, that might endanger the individual or any other person. Moreover, everything should be done in the first instance to obtain the individual's consent to the disclosure of his or her personal data. Should consent not be forthcoming, the answer to the question whether it may be appropriate and lawful to process the individual's personal data through SCIS would also depend on the identity of the contact person(s) to whom this data would be disclosed and on the specific purpose of such disclosure. Ordinarily, the proper channel of inquiry will be direct bilateral communications between the two States concerned.

5. Special safeguards may need to be included in SCIS contracts with clients and sub-contractors in view of the fact that personal data generally does not enjoy the same legal protection in other parts of the world as it does in the EU. Such safeguards could also ensure that any European Commission funding of SCIS would not inadvertently undermine the letter, object and purpose of the Treaty establishing the European Community, article 286 (ex-article 213b) of which provides that:

   "From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty."

B. Protection of personal security

1. An information request should not be processed if this would result in a reasonably foreseeable risk to the security of any person, whether associated with SCIS or not. A responsibility and, as the case may be, legal duty of care is owed to:

    - The individual with respect to whom the request is made, and his or her relatives and associates;
    - SCIS staff and contact persons, and their relatives and associates;
    - Humanitarian personnel in general;*
    - Other persons as applicable.

2. In some country situations, it might be safest for SCIS not to process any personal data at all.

_____

* Note the duty to ensure the safety and security of United Nations and associated personnel stipulated in article 7 of the *UN Convention on the Safety of United Nations and Associated Personnel*, 1994.

C. Answering the information request in the field

1. Standard operating procedures should incorporate a comprehensive and explicit protocol for interviewing contact persons. This protocol should include as a minimum the following points:

    - The interview should be held in private, so that any personal data disclosed to the contact person is not disclosed to other persons as well, and so that the contact person is able to speak as freely as possible without being influenced by others;
    - Staff should introduce themselves and explain SCIS and the purpose of the interview;
    - In explaining the purpose of the interview, it should be made explicit that the answers given may be tendered in evidence in legal proceedings in a foreign country, and that it is important that the contact person answers truthfully;
    - The contact person should give his or her consent for the interview to proceed, and be asked whether he or she consents to his or her answers being used in legal proceedings and to his or her identity being disclosed to the parties concerned;
    - Staff should be careful not to ask leading questions or to inadvertently influence answers in any other way, regardless of time or any other pressures;
    - The contact person should sign his or her statement to confirm that it is true to the best of his or her knowledge and to impress upon him or her a sense of accountability for its content;
    - Contact persons should not be remunerated, either in cash or in kind, except in payment of any standard administrative fees for official services lawfully rendered (e.g. State notary services), or in reimbursement of any legitimate expenses incurred (e.g. travel expenses of private persons).

2. SCIS sub-contractors and their staff should be selected so as to eliminate as far as possible any risk of them being exposed to undue pressures or conflicts of interest.

D. Application of the response to the information request

1. SCIS methodology should be based on the principle of "equality of arms". The identity of the contact person should be disclosed either to both the client and the applicant, or to neither. Since SCIS responses to information requests are meant to be obtained exclusively from "open sources", disclosure should be the norm.

2. In exceptional cases, a client may seek unilateral disclosure of a contact person's identity. Any decision to release the identity of the contact person only to the client, and not to the applicant as well, could only be on security grounds and should be clearly motivated and be subject to independent review.

3. If the client is unable to use a response to an information request because the identity of the contact person is non-disclosable, the client may still be able to use the response as an indicator for seeking out a source which is disclosable.

4. The evidential weight of SCIS responses to information requests should be assessed with caution, particularly if the response relates to a material issue, such as the identity of the applicant.

5. Public scrutiny can be a useful means of quality control and responses to information requests which do not contain personal data should therefore be made publicly available on the SCIS website. UNHCR previously recommended publication of SCIS responses to information requests in the specific context of the SCIS draft project proposal for Afghanistan, and welcomes the fact that SCIS has agreed to this providing that clients agree as well.

6. If SCIS engaged in fact-finding, instead of merely acting as an intermediary between contact persons and clients, this could increase the evidential weight of SCIS responses to information requests. In many cases, it could also make the disclosure of the identity of contact persons unnecessary.

Protection Information Section
Department of International Protection
UNHCR Geneva
May 2003

Annex 1

ICMPD – IES Meeting: UNHCR, HQ, 7TH June, 2002
(UNHCR, ICMPD and UK Home Office)

Participants for **UNHCR**:
Raymond Hall, Director, Bureau for Europe (Chair)
Wilbert van Hövell, Deputy Director, Dept. of International Protection
Hugh Massey, Information and Research Officer, Protection Information Section, Dept. of International Protection
Grainne O'Hara, Legal Adviser, Protection Policy and Legal Advice Section, Dept. of International Protection
Michael Petersen, Senior Legal Adviser, Bureau for Europe.

Participants for **the United Kingdom**:
Nick Swift, Immigration and Nationality Directorate,
Tom Wilkie, Assistant Director, Appeals Group, Home Office

Participants from **ICMPD-IES**:
Gottfried Zuercher, Deputy Director General, ICMPD
Nicolaas de Zwager, Programme Co-Ordinator, IES
Jean Lanoue, Head of Legal Department, IES
Werner Wendt, ICMPD-IES Head of Liaison Unit

The meeting was convened to discuss UNHCR's protection concerns relating to the implementation of ICMPD – IES field components. ICMPD expressed the wish that the meeting could reach a common understanding on the workings of the IES and its impact on RSD, in addition to establishing a mode of co-operation between UNHCR and ICMPD

Mr Hall opened the meeting, welcomed all participants, and requested a brief presentation of the actual operational features of the IES. Mr. Zuercher thanked the UNHCR for this meeting and stated his view that the objective of the meeting should be to ensure that UNHCR has a clear understanding of the IES programme and its potential impact. UNHCR and all other participants recognized the need for pertinent and objective country of origin information in many aspects of migration-related activities carried out by sovereign states, and that the IES could be one instrument, among others to obtain such information.

Mr de Zwager presented a condensed introduction of the IES programme, its primary functions and outcomes, and touched upon some key operational norms and safeguards.

UNHCR queried whether participating countries would use the IES for refugee determination in regard to Sri Lanka. IES answered that it was most likely that they would, though ICMPD estimates that this particular caseload would represent a minority of the total information requirements for Sri Lanka, with more queries relating to other matters such as return facilitation, pre-screening of visa applicants, and other COI uses.

UNHCR highlighted the fact that there are many aspects of the IES model which do not cover political or human rights related issues and are therefore essentially non-controversial with respect to protection concerns. UNHCR concerns are concentrated mainly on RSD related queries, in particular those that involve the sharing of personal data of individual applicants, including with the authorities of the country of alleged persecution.

Subsequent discussions therefore concentrated on the issues that were raised by UNHCR as being of concern (although IES made it clear it has no or limited direct control on the fourth point below):

-Quality control over the accuracy of the information
-Extent of transfer of personal data
-Safeguards followed in such cases
-Subsequent application of the information in RSD procedures.

The stated goal of UNHCR is to ensure a protection sensitive system from the outset – given its statutory responsibility but also as a pre-condition for UNHCR contemplating involvement of some sort in the IES. The test for UNHCR is not whether national legislation allows for the processing of the information or whether the IES matches or surpasses current practices, including existing embassy mechanisms. Rather, the test, as defined by UNHCR, was whether such information has been gathered in a manner, which does not put in jeopardy the security of asylum-seekers and their family and associates, in addition to UNHCR staff. Such risks arise in particular when personal data is shared directly with the authorities of countries of origin (the possibility of which ICMPD did not preclude), or comes to their knowledge, for example through the possibility of the staff of the field-based implementing partners coming under pressure. UNHCR believes that avoiding such risks would also be in the interests of the countries where asylum is sought.

UNHCR suggested that an independent evaluation of the IES (Kosovo component/KIP) should be carried out in order to more accurately gauge its impact as well as the protection sensitive nature of its field work in terms of gathering information (be this identity, nationality or other information) pertaining to specific asylum-seekers.

UNHCR offered to thoroughly examine the documents provided by ICMPD, including the various IES Terms of Reference, Standard Operating Procedures, standard contracts and guidelines, the field structure for the implementation of the project, criteria for recruitment of staff in particular in regard to safeguards. While most of these documents are already familiar to UNHCR, primarily by means of its ongoing participation in the regular IES Board meetings, it was agreed that ICMPD would compile all of the project safeguards in one document to facilitate review. UNHCR urged that this include practical information about field-based safeguards in addition to those undertaken in Vienna.

IES reiterated its long-standing invitation to UNHCR to visit the IES Central Unit. This would foster a fuller understanding of the technical nature of IES methodologies and processes that would in turn allow UNHCR to provide more targeted advice about the project. UNHCR highlighted familiarity gained from two years of experience in the field in Kosovo but agreed nonetheless that a visit to the IES Central Unit would be helpful.

Several issues relating to the IES methodology were raised and explained by IES. These related to: the consultative and open nature of feasibility studies; the selection process of a field-based implementing partner; the role of that partner; as well as the actual investigation process of certain type of requests.

Conclusions and Action Points:

It was agreed mainly to focus on and co-operate towards directly addressing the concerns UNHCR has in the implementation of IES with respect to questions that involve personal data.

In this regard it was agreed to examine the processes of the IES in detail and to consider strengthening these where possible. It was agreed that IES will provide UNHCR with a comprehensive list of the current IES safeguards, checks and balances, with specific emphasis on the handling of personal data in the field. The IES will indicate where the relevant excerpts appear in its existing documentation (Contracts, SOP, TOR, etc.) and will show also how the structure set up at the field level to implement the project and criteria for staff recruitment have regard to the need to avoid the risks giving rise to UNHCR's concerns. Ensuring that operational procedures eliminate any such risks would be a pre-condition for UNHCR contemplating any involvement at the field level.

UNHCR agrees to comment on current IES safeguards, in particular as they apply to fieldwork.

Participants looked forward to continue these positive discussions.

The UK delegation made clear that they would welcome any suggestions for further procedural safeguards. Proposed changes would be incorporated into IES procedures if considered appropriate by ICMPD and the IES Client Governments.

The content of this meeting report has been agreed to by UNHCR, ICMPD and all other participants.

July 22, 2002.

Annex 2

Selected list of international instruments concerning the processing of personal data and/or the right to privacy

United Nations: International Covenant on Civil and Political Rights (1966, article 17);[100] Convention on the Rights of the Child (1989, article 16); Universal Declaration of Human Rights (1948, article 12); Proclamation of Teheran (1968, paragraph 18); Declaration on the Human Rights of Individuals Who are Not Nationals of the Country in Which They Live (1985, article 5(1)(b)); Guidelines for the Regulation of Computerized Personal Data Files, (1990); UNHCR ExCom Conclusion No. 91 (LII) (2000) on Registration of Refugees and Asylum Seekers.

OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

Council of Europe: European Convention for the Protection of Human Rights and Fundamental Freedoms (1950, article 8); Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981); Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (2001).

European Union: Treaty establishing the European Community (article 286 – ex-article 213b); Treaty on the European Union (article F); Charter of Fundamental Rights of the European Union (2000, article 8); Convention determining the Strate responsible for examining applications for asylum lodged in one of the Member States of the European Communities (Dublin Convention, 1997); Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention; Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention; Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third country national; Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies on the free movement of such data; Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of data to processors established in third countries, under Directive 95/46/EC.

[100] See further General Comment No. 16 (1988) of the UN Human Rights Committee.